ИКАО

Doc 10213 – Unrestricted

Глобальный обзор рисков в области кибербезопасности

Издание первое, 2025

Утверждено Генеральным секретарем и опубликовано с его санкции

МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ

ИКАО

Doc 10213 – Unrestricted

Глобальный обзор рисков в области кибербезопасности

Издание первое, 2025

Утверждено и опубликовано с санкции Генерального секретаря

МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ГРАЖДАНСКОЙ АВИАЦИИ

Опубликовано отдельными изданиями на русском, английском,
арабском, испанском, китайском и французском языках
МЕЖДУНАРОДНОЙ ОРГАНИЗАЦИЕЙ ГРАЖДАНСКОЙ АВИАЦИИ.
999 Robert Bourassa Boulevard, Montréal, Quebec, Canada H3C 5H7

Информация о порядке оформления заказов и полный список агентов по
продаже и книготорговых фирм размещены на веб-сайте ИКАО www.icao.int.

Издание первое, 2025 год.

Doc 10213. ***Глобальный обзор рисков в области кибербезопасности***
Номер заказа: 10213-U
ISBN 978-92-9275-973-5

ПОПРАВКИ

Об издании поправок сообщается в дополнениях к Каталогу ИКАО *"Продукция и услуги"*; каталог и дополнения к нему размещены на веб-сайте ИКАО www.icao.int. Ниже приведена таблица для регистрации поправок.

РЕГИСТРАЦИЯ ПОПРАВОК И ИСПРАВЛЕНИЙ

ПОПРАВКИ		
№	Дата	Кем внесено

ИСПРАВЛЕНИЯ			
№	Язык	Дата	Кем внесено

Документ ИКАО *"Глобальный обзор рисков в области кибербезопасности"* (Doc 10213 – Restricted) содержит информацию для служебного доступа и предназначен для ограниченного использования государственными, отраслевыми и другими заинтересованными сторонами в области авиации, участвующими в обеспечении кибербезопасности, в целях оценки рисков. Данная редакция документа Doc 10213 содержит выдержки из общедоступных разделов и подготовлена для публичного распространения.

ПРЕДИСЛОВИЕ

В последние два десятилетия происходит стремительная эволюция в использовании информации и новых технологий в секторе гражданской авиации для поддержки целей автоматизации, взаимосвязанности и интероперабельности. В последнее время эта тенденция ускоряется, особенно в эксплуатационных областях, что вызвано стремлением извлечь выгоду из последних технологических достижений, таких как машинное обучение и анализ больших данных. Цифровизация ускорит развертывание новых эксплуатационных концепций на земле и в воздухе и позволит интегрировать в систему воздушного транспорта новых участников воздушного движения, таких как беспилотные авиационные системы (БАС). Конечной целью этих изменений является поддержка роста сектора гражданской авиации, а также обеспечение его безопасности, надежности, эффективности, пропускной способности и устойчивости.

В то же время эта тенденция привела к расширению спектра киберугроз, которым теперь подвергаются эксплуатационные системы и информация, что может оказать негативное воздействие на безопасность полетов, авиационную безопасность, пропускную способность и/или эффективность гражданской авиации. В результате авиационный сектор оказался вынужден бороться с киберугрозами и рисками для гражданской авиации, выходящими за пределы традиционного контекста безопасности информационных технологий/ эксплуатационных технологий (ИТ/ЭТ), при этом управление киберрисками в авиации должно быть интегрировано в процессы управления авиационными рисками во всех отраслях гражданской авиации. Это делается для обеспечения защищенности и устойчивости системы воздушного транспорта с помощью эффективных и надежных систем управления рисками.

Документ *"Глобальный обзор рисков в области кибербезопасности"* был разработан Международной организацией гражданской авиации (ИКАО) в целях оказания государствам-членам и заинтересованным сторонам поддержки в интеграции управления киберрисками в их процессы управления рисками в авиации. Кроме того, в нем представлен общий глобальный обзор киберугроз, с тем чтобы подчеркнуть важность устранения киберугроз и рисков для гражданской авиации в интересах обеспечения устойчивости и защищенности сектора.

Данный документ призван оказать поддержку государствам и заинтересованным сторонам в выполнении ими своих обязательств по оценке рисков; эти обязательства закреплены в Приложениях к Конвенции о международной гражданской авиации (Чикагская конвенция), в частности в Стандарте 4.9.1 Приложения 17 *"Авиационная безопасность"*. Этот документ также способствует реализации Стратегии ИКАО в области авиационной кибербезопасности[1] и связанного с ней Плана действий по обеспечению кибербезопасности[2].

Информация, содержащаяся в настоящем документе, соответствует общим принципам инструктивных материалов ИКАО по оценке рисков для безопасности полетов и авиационной безопасности и по процессам управления, изложенным в *Заявлении о глобальном контексте риска в области авиационной безопасности* (Doc 10108 – Restricted), *Руководстве по авиационной безопасности* (Doc 8973 – Restricted) и *Руководстве по управлению безопасностью полетов* (Doc 9859).

Этот документ также включает в себя добавления, в которых приведены примеры применения методики управления киберрисками при оценке рисков в области безопасности полетов и авиационной безопасности. В добавлениях содержатся также рекомендации по классификации киберугроз, призванные помочь государствам и заинтересованным сторонам выявлять взаимозависимости и связи между различными авиационными отраслями. Цель заключается в содействии разработке и поддержанию надежной системы управления рисками в гражданской авиации.

Мы хотели бы выразить признательность экспертам Группы экспертов по кибербезопасности и ее Рабочей группы по киберугрозам и рискам за их ценный вклад в виде времени и знаний, позволивших разработать этот документ.

---

1. См. https://www.icao.int/aviationcybersecurity/Pages/Aviation-Cybersecurity-_Strategy.aspx
2. См. https://www.icao.int/aviationcybersecurity/Pages/Cybersecurity-Action-Plan.aspx.

СОДЕРЖАНИЕ

СОКРАЩЕНИЯ И АКРОНИМЫ

БАС	Беспилотная авиационная система
ИТ/ЭТ	Информационные технологии/эксплуатационные технологии
ОВКВ	Отопление, вентиляция и кондиционирование воздуха
ПАНО	Поставщик аэронавигационного обслуживания
УВД	Управление воздушным движением
APT	Продвинутая постоянная угроза
AVSEC	Авиационная безопасность
CPDLC	Связь "диспетчер – пилот" по линии передачи данных
CRC	Контроль с использованием циклического избыточного кода
DDoS	Распределенная атака типа "отказ в обслуживании"
EATM-CERT	Группа реагирования на компьютерные инциденты Европейской системы организации воздушного движения
EFB	Электронный полетный планшет
FTA	Анализ дерева отказов
GNSS	Глобальная навигационная спутниковая система
IP	Протокол сети Интернет
IPR	Право интеллектуальной собственности
MET	Метеорологический
NEASCOG	Координационная группа по авиационной безопасности при организации воздушного движения (ОрВД) НАТО/ЕВРОКОНТРОЛЯ
PBIED	Самодельное взрывное устройство, перевозимое человеком
PII	Информация, позволяющая установить личность человека

Глава 1

ОПРЕДЕЛЕНИЯ

Авиационная кибербезопасность. Комплекс технологий, средств контроля и мер, а также процессов и практических методов, предназначенных для обеспечения конфиденциальности, целостности, доступности и общей защиты систем, сетей, программ, устройств, информации и данных от атак, повреждений, несанкционированного доступа, использования и/или эксплуатации.

Вектор атаки. Средства доступа, которые злоумышленник использовал для начала атаки.

Готовность к работе. Показатель доступности и пригодности для использования по требованию уполномоченного лица, пользователя, программы, процесса, системы или устройства.

Киберактив. Цифровые и физические объекты, имеющие ценность с точки зрения деловой деятельности, производства полетов, безопасности полетов, авиационной безопасности, эффективности и/или пропускной способности, такие как системы, информация, данные, сети, устройства, программное обеспечение, аппаратные средства, процессы, встроенное программное обеспечение, соответствующий/сертифицированный персонал и другие электронные ресурсы.

Кибератака. Преднамеренное использование электронных средств для прерывания работы, изменения, уничтожения киберактивов или получения несанкционированного доступа к ним.

Киберинцидент. Разовое киберсобытие или серия киберсобытий, которые отрицательно сказываются на безопасности полетов, авиационной безопасности, эффективности и/или пропускной способности.

Киберриск. Возможность нежелательных последствий киберсобытия.

Киберсобытие. Любое наблюдаемое событие в сети или системе.

Киберугроза. Любое потенциальное киберсобытие, которое может отрицательно сказаться на безопасности полетов, авиационной безопасности, эффективности и/или пропускной способности.

Киберустойчивость. Способность киберактива обеспечивать выполнение важнейших функций в неблагоприятных условиях или при увеличенной нагрузке и восстанавливаться после таких неблагоприятных условий.

Контроль доступа. Меры, призванные обеспечить предоставление только санкционированного доступа к физическим и киберактивам.

Конфиденциальность. Принцип, согласно которому актив не предоставляется или не раскрывается лицу, пользователю, программе, процессу, системе или устройству, не имеющему соответствующего разрешения.

Критическая авиационная инфраструктура. Активы, значение которых настолько велико, что их непригодность к работе, нарушение их безопасности или их разрушение привели бы к губительным последствиям для безопасности полетов, авиационной безопасности, эффективности и/или пропускной способности.

Матрица киберрисков. Инструмент для ранжирования и отображения компонентов рисков (вероятности, угрозы, воздействия/последствий и уязвимости), способов устранения последствий и в конечном итоге остаточных факторов риска.

Надежность. Свойство актива, предполагающее, что при определенных условиях в течение определенного периода времени он будет выполнять требуемую функцию на ожидаемом уровне без сбоев.

Нарушение нормальной работы. Ожидаемое или непредвиденное киберсобытие, которое приводит к незапланированному негативному отклонению от нормальной работы.

Оценка киберрисков. Непрерывный процесс выявления, анализа и оценки киберрисков.

Снижение риска кибератаки. Средства контроля за безопасностью, направленные на снижение киберриска, связанного с конкретной киберугрозой или уязвимостью, с учетом их воздействия на безопасность полетов, авиационную безопасность, эффективность и/или пропускную способность.

Субъект угрозы. Субъект, частично или полностью ответственный за инцидент, который воздействует (или может воздействовать) на организацию или систему.

Тяжесть последствий. Качественный показатель величины неблагоприятных последствий угрозы.

Управление киберрисками. Непрерывный процесс выявления, уменьшения последствий, урегулирования и мониторинга киберугроз и рисков в соответствии с оценкой рисков.

Целостность. Свойство, гарантирующее точность и полноту актива и подтверждающее, что актив представляет собой то, чем он заявлен.

Глава 2

МЕТОДОЛОГИЯ ИНТЕГРАЦИИ УПРАВЛЕНИЯ КИБЕРРИСКАМИ В СИСТЕМЫ УПРАВЛЕНИЯ РИСКАМИ В АВИАЦИИ

Примечание 1. В данной главе под авиационными функциями понимаются функции в рамках различных авиационных дисциплин (авиационной дисциплины), в которых (которой) управление киберрисками интегрировано в предусмотренные ими (ею) процессы управления рисками, а именно: безопасность полетов, авиационная безопасность, аэронавигационная эффективность и/или пропускная способность аэронавигации. В том же контексте под критически важными авиационными функциями понимаются функции, которые считаются критически важными для соответствующей авиационной дисциплины (дисциплин).

Примечание 2. В данной главе под специалистами по управлению авиационными рисками понимаются специалисты в области безопасности полетов, авиационной безопасности, аэронавигационной эффективности и/или управления рисками для пропускной способности, в то время как процессы управления авиационными рисками означают процессы управления рисками в соответствующей авиационной дисциплине (дисциплинах).

2.1 ЦЕЛИ

2.1.1 Данная глава призвана оказать поддержку государствам и заинтересованным сторонам в их процессах управления рисками, от выявления рисков до их обработки и пересмотра, и в этих целях содержит общую методологию интеграции оценки и управления киберрисками в существующие системы управления рисками в области безопасности полетов, авиационной безопасности, аэронавигационной эффективности и пропускной способности.

Примечание 1. Несмотря на то, что методология предусматривает интеграцию управления киберрисками в оценку рисков для безопасности полетов, авиационной безопасности, аэронавигационной эффективности и пропускной способности, она может быть адаптирована для применения к любой другой дисциплине гражданской авиации (например, к управлению деловыми рисками).

Примечание 2. Прежде чем применять методологию, изложенную в данной главе, государства и заинтересованные стороны, возможно, пожелают принять во внимание области, в которых существующие методологии оценки рисков широко признаются компетентными органами в качестве приемлемых средств соблюдения их конкретных нормативных требований для авиации, например в случае оценки рисков, связанных с сертификацией воздушных судов.

2.1.2 Данная глава адресована специалистам в области управления безопасностью полетов, авиационной безопасностью, аэронавигацией и киберрисками, которым следует работать совместно над интеграцией управления киберрисками в свои соответствующие системы управления авиационными рисками в рамках всех дисциплин гражданской авиации.

2.2 ОБЩАЯ ИНФОРМАЦИЯ

2.2.1 Методология, представленная в настоящем документе, соответствует общим концепциям эффективного цикла управления рисками, отраженного на рис. 1.

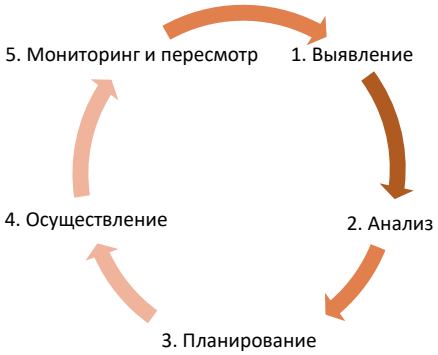


Рис. 1. Цикл управления рисками

2.2.2 Данная методология опирается на существующие инструктивные материалы ИКАО по оценке рисков, а именно на *Руководство по управлению безопасностью полетов* (Doc 9859) и *Заявление о глобальном контексте риска в области авиационной безопасности* (Doc 10108 – Restricted). В ней учтена работа различных экспертных групп ИКАО, а также вклад Координационной группы по авиационной безопасности при организации воздушного движения (ОрВД) НАТО/ЕВРОКОНТРОЛЯ (NEASCOG). Помимо этого, она соответствует международным стандартам по управлению киберрисками (ISO/IEC 27001:2022[3], ISO 31000:2018[4], EUROCAE/RTCA ED-201A/DO-391[5] и NIST SP 800-30 Rev.1[6]).

2.2.3 Применение данной методологии к существующим оценкам авиационных рисков, связанных с критически важными авиационными функциями, будет иметь следующие результаты:

- обновленная оценка рисков для безопасности полетов, включающая в себя оценку соответствующих киберрисков;
- обновленная оценка рисков для авиационной безопасности, включающая в себя оценку соответствующих киберрисков;
- обновленная оценка рисков для эффективности аэронавигации, включающая в себя оценку соответствующих киберрисков; и/или
- обновленная оценка рисков для пропускной способности аэронавигации, включающая в себя оценку соответствующих киберрисков.

2.2.4 Прежде чем применять рассматриваемую методологию, важно, чтобы специалисты в области авиации определили важнейшие авиационные функции в дисциплине, в отношении которых проводится оценка. Это может быть достигнуто путем консультаций, опросов и т. д. с учетом нормативных и законодательных требований, применимых как к авиации, так и к национальной критически важной инфраструктуре.

Примечание. Определение критически важных авиационных функций и их вспомогательных данных, информации и систем в сочетании с применением данной методологии помогает государствам в их усилиях по выполнению своих обязательств в соответствии со Стандартом 4.9.1 Приложения 17 "Авиационная безопасность"[7].

3. См. https://www.iso.org/standard/27001.
4. См. https://www.iso.org/standard/65694.html.
5. См. https://www.eurocae.net/product/ed-201a-aeronautical-information-system-security-aiss-framework-guidance/ или https://www.rtca.org/security/.
6. См. https://csrc.nist.gov/pubs/sp/800/30/r1/final.
7. Приложения к Чикагской конвенции, включая Приложение 17 и содержащийся в нем Стандарт 4.9.1, применимы к государствам, а не к отдельным авиационным дисциплинам, если не указано иное. В Стандарте 4.9.1 говорится об "эксплуатантах или организациях, указанных в национальной программе безопасности гражданской авиации или другой авиационным дисциплинам, определяемым каждым государством на национальном уровне.

2.2.5 Методология, схематично изображенная на рис. 2 ниже, должна включать в себя изложенные далее этапы.

- **Этап 1.** *Этот этап должен быть реализован специалистами по соответствующим авиационным рискам в сотрудничестве со специалистами по кибербезопасности.*
  - ⇨ Начать с существующей оценки авиационных рисков для критически важной авиационной функции.
  - ⇨ По результатам оценки авиационных рисков будут установлены:
    - минимальный допустимый уровень безопасности полетов, называемый целевым уровнем безопасности полетов;
    - остаточный риск для авиационной безопасности;
    - минимальный целевой уровень пропускной способности; и/или
    - минимальный целевой уровень эффективности.
  - ⇨ Выявить данные, информацию и системы, которые поддерживают соответствующую критически важную авиационную функцию и вмешательство в которые может повлиять на безопасность полетов, авиационную безопасность, эффективность и/или пропускную способность гражданской авиации.

Примечание. В случае выявления критически важной авиационной функции, для которой отсутствует оценка авиационных рисков, следует провести соответствующую оценку рисков для авиации и использовать её на этапе 1. Одновременно с этим может быть реализован этап 2, описанный ниже, для оценки рисков для данных, информации и систем, поддерживающих эту функцию.

- **Этап 2.** *Этот этап должен быть реализован специалистами по кибербезопасности в сотрудничестве со специалистами по соответствующим авиационным рискам.*
  - ⇨ Определить сценарии киберугроз, способные повлиять на обозначенные выше данные, информацию и системы, и провести оценку киберрисков в рамках этих сценариев.
    - Описать сценарий угрозы, включая средства и методы кибератаки, а также тип субъекта угрозы.
    - Вероятность сценария должна быть сначала оценена без учета предусмотренных на данный момент мер по снижению риска. Оценке подлежит намерение субъекта угрозы и его способность реализовать сценарий угрозы. Этот этап может включать в себя, по возможности, описание профиля субъекта угрозы, его инструментов и т. д.

Примечание. В отношении выявленных киберугроз должен осуществляться постоянный контроль, с тем чтобы учитывать изменения в намерениях и/или возможностях субъектов угроз.

- Воздействие/последствия/эффект[8] оцениваются с точки зрения характера и масштаба конкретной атаки по отношению к безопасности полетов, авиационной безопасности, пропускной способности аэронавигации и/или аэронавигационной эффективности при разумном наихудшем сценарии или наихудшем вероятном сценарии.
- В оценке сохраняющихся факторов уязвимости системы учитывается реализация существующих мер по смягчению последствий.
- Результатом обозначенной выше оценки является остаточный киберриск. Он представляет собой общий риск, сохраняющийся после того, как были проанализированы применяемые меры по снижению риска и были приняты во внимание вероятность угрозы и ее последствия.

Примечание 1. Таблицы ранжирования вероятности, воздействия и сохраняющихся факторов уязвимости описаны в следующем разделе.

Примечание 2. Каждой организации следует определить свои собственные цели в области кибербезопасности и критерии принятия киберрисков с опорой на нормативно-правовую базу, регулирующую авиационную и неавиационную сферы (например, действующую в отношении национального ведомства по кибербезопасности), а также на собственные допустимые уровни риска.

8. В настоящем документе понятия "воздействие", "последствия" и "эффект" используются как взаимозаменяемые синонимы.

➢ **Этап 3.** *Этот этап должен быть выполнен специалистами по авиационным рискам.*

⇨ Обновить оценку авиационных рисков, предусмотренную на этапе 1. Результатом работы на этом этапе будут:

- обновленный уровень безопасности полетов;
- обновленный остаточный риск для авиационной безопасности;
- обновленный уровень пропускной способности; и/или
- обновленный уровень эффективности.

➢ **Этап 4.** *Этот этап должен быть реализован специалистами по авиационным рискам в сотрудничестве со специалистами по кибербезопасности.*

⇨ Оценить результаты обновленной оценки авиационных рисков в сравнении с исходными уровнями риска, полученными на этапе 1.

⇨ Критерии принятия риска должны быть заранее определены организацией и должны быть всеобъемлющими, охватывая по меньшей мере соответствующие авиационные дисциплины (безопасность полетов, авиационную безопасность, пропускную способность и/или эффективность) и задачи и целевые показатели в области кибербезопасности.

Примечание. Каждой организации следует определить свои собственные критерии принятия рисков с опорой на нормативно-правовую базу, регулирующую авиационную (и в некоторых случаях неавиационную) сферу, а также на собственные допустимые уровни риска.

⇨ После оценки обновленных результатов в сравнении с исходными результатами, полученными на этапе 1, пересмотренный уровень риска в рамках оценки авиационных рисков должен быть признан неприемлемым, если:

- обновленная оценка авиационного риска не соответствует принятым целевым показателям (исходным уровням риска), полученным на этапе 1; или
- остаточный киберриск не соответствует задачам организации в области кибербезопасности.

⇨ Если обновленный уровень риска неприемлем, организации следует снизить риск, добавив конкретные меры по снижению рисков для кибербезопасности там, где это возможно, и пересмотреть приемлемость этого риска.

⇨ Если даже после внедрения мер по снижению рисков для кибербезопасности уровень риска по-прежнему остается неприемлемым, организации следует определить другие новые, релевантные и эффективные меры по снижению риска до приемлемого уровня.

Примечание. В случае возникновения конфликта в отношении приемлемости риска между авиационными и киберспециалистами, вопрос следует передать на рассмотрение руководящему звену организации.

⇨ Если планируются меры по снижению рисков для кибербезопасности, следует вернуться к этапу 3.

⇨ Убедиться в том, что новые меры по снижению рисков для кибербезопасности не оказывают негативного влияния на оценку авиационных рисков. При необходимости принять авиационные меры[9] или пересмотреть меры в области кибербезопасности для устранения любого негативного воздействия.

Примечание. Важно учитывать потенциальное влияние мер по снижению рисков для кибербезопасности на критически важные данные, информацию и/или системы других критически важных авиационных функций, поскольку такие меры могут повлиять на эти функции. В случае выявления такого влияния следует провести совместную оценку авиационных и киберрисков, связанных с этими критически важными функциями.

⇨ Оценку следует повторить при наличии следующих причин:

- эволюция киберугроз, например существующих или новых сценариев киберугроз, которые со временем могут стать вероятными, изменения в информации или знаниях, используемых для идентификации, анализа и классификации рисков;

9. Под авиационными мерами понимаются меры по обеспечению безопасности полетов, авиационной безопасности, эффективности аэронавигации и/или эксплуатационные меры для обеспечения пропускной способности.

- изменения в требованиях, связанных с оценкой рисков в дисциплине (дисциплинах), в которую (которые) интегрируются киберриски;
- функциональные изменения в оцениваемых авиационных функциях; и/или
- изменения в параметрах приемлемого риска организации и политике в отношении непрерывного мониторинга и оценки и/или повторение оценки рисков.

2.2.6 В добавлениях A и B приведены два примера того, как описанная методология может быть применена на практике. Первый пример, описанный в **добавлении A**, показывает, как интегрировать киберугрозу в оценку рисков для безопасности полетов. Второй пример, описанный в **добавлении B**, показывает, как киберугроза может быть интегрирована в оценку рисков для авиационной безопасности.

2.2.7 Цель этих примеров состоит в том, чтобы продемонстрировать, что оценки авиационных рисков и оценки киберрисков не могут проводиться изолированно, если рассматриваются киберугрозы для авиационных процессов. **Для обеспечения комплексной защиты и устойчивости гражданской авиации к киберугрозам и рискам чрезвычайно важно обеспечить взаимодействие, координацию и сотрудничество при проведении этих оценок.**

2.3 СХЕМА ПРЕДУСМОТРЕННОГО МЕТОДОЛОГИЕЙ ПРОЦЕССА И ТАБЛИЦЫ БАЛЛЬНОЙ ОЦЕНКИ КИБЕРРИСКОВ

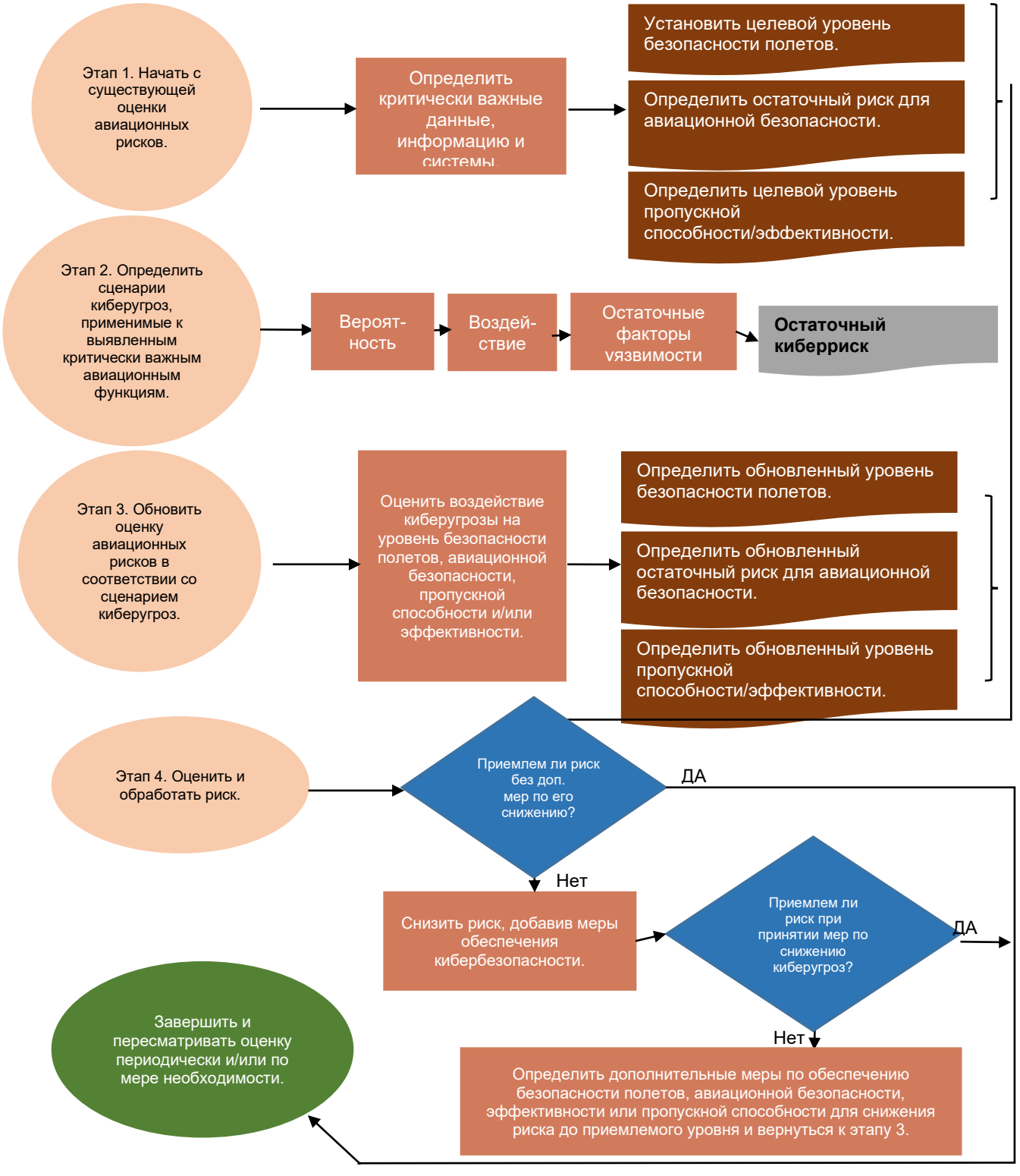


Рис. 2. Методология управления рисками: схема процесса

Таблицы балльной оценки киберрисков

2.3.1 Разные таблицы балльной оценки рисков, приведенные в этом разделе, служат примером передовой практики и инструктивной информацией по построению матриц оценки киберрисков. Несмотря на то, что использование этих таблиц балльной оценки рисков рекомендуется для обеспечения взаимного понимания киберугроз и рисков в контексте обмена информацией [10], они могут быть адаптированы в соответствии с существующими у организаций стратегиями управления рисками.

2.3.2 Баллы, приведенные в этом разделе, используются для составления оценок, которым посвящена глава 3 настоящего документа в редакции для служебного пользования.

2.3.3 В рамках данной методологии вероятность, влияние и уязвимость ранжируются по пяти уровням (ВЫСОКИЙ, СРЕДНЕ-ВЫСОКИЙ, СРЕДНИЙ, СРЕДНЕ-НИЗКИЙ, НИЗКИЙ). Каждому уровню соответствует балл и дано определение.

Вероятность

2.3.4 Под вероятностью понимается возможность реализации киберугрозы с учетом наличия у субъекта угрозы способности и намерения провести такую кибератаку.

2.3.5 Оценка вероятности должна проводиться экспертами по кибербезопасности или по крайней мере экспертами по соответствующим авиационным рискам, имеющими доступ к аналитическим отчетам о киберугрозах.

Таблица 1. Ранжирование вероятности киберугроз

УРОВЕНЬ ВЕРОЯТНОСТИ РЕАЛИЗАЦИИ РИСКА		
ВЫСОКИЙ	5	Весьма вероятный сценарий, когда нападения такого рода имели место в последние несколько лет либо существуют весомые доказательства наличия способности и намерения его осуществить.
СРЕДНЕ-ВЫСОКИЙ	4	Явно вероятный сценарий, свидетельством чему служат относительно недавно имевшие место примеры или доказательства заблаговременного планирования нападения или ведения наблюдения со злонамеренными целями.
СРЕДНИЙ	3	В большой степени вероятный сценарий, так как имеются некоторые сведения о намерениях и способности совершить нападение, и, возможно, есть некоторые примеры таких нападений.
СРЕДНЕ-НИЗКИЙ	2	Сценарий, примеров которому не существует или нет в практике последнего времени, однако в отношении которого имеются некоторые сведения о намерениях его осуществить, хотя, по всей видимости, методика для успешной реализации нападения отработана еще недостаточно и вполне вероятно, что предпочтение будет отдано другой форме совершения нападения.

10. Для получения дополнительной информации об обмене киберинформацией см. инструктивный материал по обмену киберинформацией по ссылке: https://www.icao.int/aviationcybersecurity/Pages/Guidance-material.aspx.

НИЗКИЙ	1	Теоретически вероятный сценарий, однако отсутствуют примеры такого нападения, и имеется теоретическое намерение, но нет явных доказательств способности к его реализации.

Воздействие/последствия/эффект

2.3.6 Воздействие является результатом качественной оценки последствий киберинцидента для активов, указанных в описании сценария угрозы.

2.3.7 Оценку воздействия должны проводить авиационные эксперты анализируемой авиационной функции.

2.3.8 Информация о воздействии на безопасность полетов и авиационную безопасность взята из инструктивных материалов ИКАО по оценке рисков для безопасности полетов и авиационной безопасности – *Руководства по управлению безопасностью полетов* (Doc 9859) и *Заявления о глобальном контексте риска в области авиационной безопасности* (Doc 10108 – Restricted) соответственно. Оценка воздействия на пропускную способность и эффективность аэронавигации была разработана для настоящего документа.

Таблица 2. Ранжирование уровней воздействия киберугроз

УРОВЕНЬ ВОЗДЕЙСТВИЯ/ПОСЛЕДСТВИЙ/ЭФФЕКТА[11]			
	Безопасность полетов[12]	**Авиационная безопасность[13]**	**Пропускная способность и/или эффективность аэронавигации**
ВЫСОКИЙ **Балл = 5**	**Катастрофические последствия** - Разрушение воздушного судна	- Сотни погибших - Миллиарды долларов США - Серьезное нарушение функциониро-вания служб и подрыв доверия к авиационной системе	- Критический сбой в пропускной способности и/или эффективности аэронавигации. - Широкомасштабные сбои в работе или полный отказ ключевых эксплуатационных систем, серьезно влияющие на организацию воздушного движения, операции в аэропортах[14] или производство полетов авиакомпаниями[15]. - Длительные задержки или отмены рейсов, создающие значительные эксплуатационные риски для авиационной системы и способности эксплуатировать воздушные суда.

11. Таблица уровней воздействия/последствий/эффекта описывает влияние для каждой авиационной дисциплины, в которой используется данная методология. Столбцы независимы друг от друга — каждый посвящен отдельной авиационной дисциплине, а баллы, указанные в первом столбце, следует рассматривать вместе со столбцом, относящимся к авиационной дисциплине, в которую интегрируется оценка киберрисков.
12. Информация о воздействии/последствиях/эффекте на безопасность полетов взята из четвертого издания *Руководства по управлению безопасностью полетов* (Doc 9859).
13. Информация о воздействии/последствиях/эффекте на авиационную безопасность взята из третьего издания *Заявления о глобальном контексте риска в области авиационной безопасности* (Doc 10108 – Restricted).
14. В данном контексте операции в аэропортах включают в себя все аэропортовые службы, необходимые для прибытия, убытия и руления воздушных судов, а также работу с пассажирами, включая, в частности, доступ к выходам на посадку, доступность услуг безопасности, осмотр взлетно-посадочной полосы, обработку багажа, топливо, удаление обледенения, бортпитание, освещение аэропорта и другие сопутствующие службы.
15. В данном контексте производство полетов авиакомпаниями включает в себя все аспекты, влияющие на способность эффективно эксплуатировать воздушные суда, включая передачу информации летным экипажам, техническое обслуживание воздушных судов, эксплуатацию воздушных судов, MET, доступность GNSS вместо неточной навигации и захода на посадку, аэронавигационную информацию и т. д.

СРЕДНЕ-ВЫСОКИЙ **Балл = 4**	**Опасные последствия:** - Серьезные телесные повреждения - Крупный ущерб - Настолько значительное уменьшение "запаса прочности безопасности", что нет уверенности в правильном или полном выполнении эксплуатационным персоналом своих задач.	- Некоторые, но не все, последствия ВЫСОКОГО уровня	- Существенный сбой в пропускной способности и/или эффективности аэронавигации. - Длительные сбои в ключевых эксплуатационных системах или их полный отказ, влияющие на основные службы и возможности эксплуатации воздушных судов. - Существенные задержки в потоке воздушного движения, операциях в аэропорту или производстве полетов авиакомпаниями, приводящие к перегруженности.
СРЕДНИЙ **Балл = 3**	**Значительные последствия:** - Телесные повреждения - Серьезный инцидент - Снижение способности эксплуатационного персонала справляться с неблагоприятными эксплуатационными условиями из-за увеличения рабочей нагрузки или вследствие условий, понижающих эффективность работы.	- Десятки погибших - Сотни миллионов долларов США - Существенное нарушение функциониро-вания служб и подрыв доверия к авиационной системе	- Заметные сбои в пропускной способности и/или эффективности аэронавигации. - Частичные перебои в функционировании ключевых эксплуатационных систем или их неисправность, влияющие на работу нескольких служб. - Умеренные задержки в потоке воздушного движения или умеренное воздействие на операции в аэропорту или производство полетов авиакомпаниями, управление которыми требует дополнительной координации и ресурсов.
СРЕДНЕ-НИЗКИЙ **Балл = 2**	**Малозначимые последствия:** - Неудобства и эксплуатационные ограничения - Использование аварийных процедур - Незначительный инцидент	- Некоторые, но не все, последствия СРЕДНЕГО уровня	- Незначительные сбои в пропускной способности и/или эффективности аэронавигации. - Ограниченный инцидент, затрагивающий отдельно взятые системы или службы. - Небольшие задержки или неэффективность в потоке воздушного движения, операциях в аэропортах или производстве полетов авиакомпаниями, с которыми можно справиться в рамках обычных эксплуатационных процедур.
НИЗКИЙ **Балл = 1**	**Несущественные последствия.** - Возможно наличие нескольких пострадавших - Ограниченные последствия	- Возможно наличие нескольких погибших и пострадавших - Небольшой экономический ущерб - Небольшое нарушение функциониро-вания служб и небольшой подрыв доверия к авиационной системе	- Несущественный сбой в пропускной способности и/или эффективности аэронавигации. - Единичный инцидент с весьма ограниченным воздействием на полеты в целом. - Весьма ограниченные задержки или сбои в потоке воздушного движения, весьма ограниченное воздействие на операции в аэропортах или на производство полетов авиакомпаниями.

Уязвимость

2.3.9 Уязвимость измеряется в качественных показателях и описывает эффективность существующих мер по смягчению последствий сценария киберугрозы для соответствующих активов.

2.3.10 Авиационным экспертам следует проводить оценку уязвимости совместно с киберэкспертами, которые могут проанализировать соответствующую критически важную авиационную функцию и оценить, каким образом субъекты угрозы могут использовать киберуязвимости.

Таблица 3. Ранжирование уровней уязвимости к киберугрозам

УРОВЕНЬ УЯЗВИМОСТИ		
ВЫСОКИЙ	1	Не принимается никаких мер по снижению уровня угрозы по причине отсутствия таких требований или отсутствия каких-либо реально осуществимых эффективных мер.
СРЕДНЕ-ВЫСОКИЙ	0,8	Меры по снижению уровня угрозы носят ограниченный характер, а важные области и аспекты риска не охватываются действующими требованиями или мерами.
СРЕДНИЙ	0,6	Присутствуют признаки как СРЕДНЕ-ВЫСОКОГО, так и СРЕДНЕ-НИЗКОГО уровней.
СРЕДНЕ-НИЗКИЙ	0,4	Меры по снижению уровня риска применяются, но либо они в недостаточной мере отработаны, либо эффективны лишь частично. Например, руководства по информационной безопасности, разработанные ИКАО, возможно, существуют для всех областей и аспектов, но или требуют дальнейшей доработки, или должны более эффективно внедряться на практике.
НИЗКИЙ	0,2	Существуют четкие требования, и широко используются меры по снижению рисков, которые в целом считаются эффективными.

Пример оценки киберриска

Таблица 4. Матрицы балльной и общей оценки киберрисков

МАТРИЦА ОЦЕНКИ КИБЕРРИСКОВ								
Сценарий киберугрозы	**Вероятность**	**X**	**Воздействие**	**X**	**Уязвимость**	**=**	**Остаточный фактор риска**
Субъект угрозы использует кибератаку для воздействия на авиационный актив, управляемый заинтересованным лицом в сфере авиации, используя уязвимость.	**СРЕДНЯЯ** **3**		**СРЕДНЕ-ВЫСОКОЕ** **4**		**СРЕДНЕ-ВЫСОКАЯ** **0,8**		**9,6**

МАТРИЦА БАЛЛЬНОЙ ОЦЕНКИ КИБЕРРИСКОВ	
БАЛЛЬНАЯ ОЦЕНКА РИСКА	**УРОВЕНЬ РИСКА**
20–25	ВЫСОКИЙ
15–20	СРЕДНЕ-ВЫСОКИЙ
10–15	СРЕДНИЙ
5–10	СРЕДНЕ-НИЗКИЙ
0–5	НИЗКИЙ

ДОБАВЛЕНИЯ

Добавление A

ПРИМЕР ПРИМЕНЕНИЯ МЕТОДИКИ В ОБЛАСТИ УПРАВЛЕНИЯ РИСКАМИ ДЛЯ БЕЗОПАСНОСТИ ПОЛЕТОВ

ДОПУЩЕНИЯ И ОБЩАЯ ИНФОРМАЦИЯ

Этот пример иллюстрирует интеграцию оценки киберрисков в оценку рисков для безопасности полетов с использованием гипотетического сценария угрозы, оцениваемого поставщиком аэронавигационного обслуживания (ПАНО).

Допущения:

- ПАНО уже провел качественную и количественную оценку рисков для безопасности полетов и снизил эти риски с помощью анализа дерева отказов (FTA)[16].
- Эксперты по безопасности полетов определили двустороннюю связь "воздух – земля" в качестве одной из критически важных авиационных функций.
- Для упрощения допускается, что оцениваемая киберугроза влияет только на безопасность полетов (и не влияет на эффективность и пропускную способность аэронавигации).
- ПАНО использует те же таблицы оценки вероятности, воздействия и уязвимости, которые использованы в данном документе.
- Для балльной оценки киберрисков используются значения, отличные от приведенных в пункте 3.3.17, поскольку объем оценки в данном примере ограничен наземными системами и данными, относящимися к CPDLC.
- Для упрощения в приведенном ниже сценарии киберугрозы, как показано на рис. 3, используется допущение, что воздействие киберугрозы распространяется только на сообщения CPDLC, связанные с диспетчерским разрешением в отношении эшелона полета.

Сценарий киберугрозы:

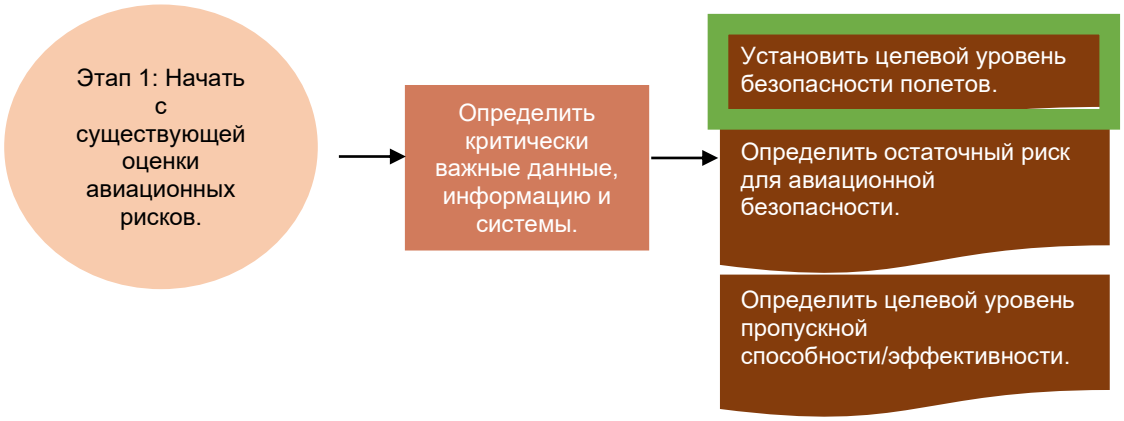
- Эксперты по безопасности полетов совместно с экспертами по кибербезопасности провели анализ существующих оценок рисков для безопасности полетов в отношении функции связи "воздух – земля" и определили CPDLC в качестве системы и информации, поддерживающей критически важную функцию, которую необходимо оценить на предмет киберрисков.
- Эксперты по безопасности полетов подготовили оценку актуальных рисков для безопасности полетов в отношении конечного события, связанного с CPDLC: "Необнаруженная несанкционированная передача одного или нескольких сообщений, использованных для предоставления диспетчерских разрешений (разрешенный эшелон полета – CFL, направление и скорость) одному или нескольким воздушным судам".
- Эксперты по кибербезопасности в ходе обсуждений с экспертами по безопасности полетов определили "искажение данных сообщения CPDLC, отправленного авиадиспетчером пилоту" в качестве сценария киберугрозы, подлежащего оценке и включению в вышеуказанную оценку рисков для безопасности полетов.
- В данном примере производится оценка сценария, охватывающего преднамеренное искажение данных сообщения CPDLC от диспетчера пилоту, при котором исходное сообщение (разрешенный эшелон полета), отправленное авиадиспетчером пилоту, подделывается (заменяется намеренно ложным эшелоном полета) злоумышленником перед его передачей на борт воздушного судна.

16. FTA – это инструмент, который поддерживает выявление и анализ условий и факторов, вызывающих возникновение или являющихся одной из причин возникновения определенного нежелательного события, обычно такого, которое существенно влияет на безопасность, производительность, экономичность или другие требуемые характеристики системы. FTA активно применяется для оценки безопасности систем.
Руководство по использованию FTA можно найти в части IV приложения K "Инструктивный материал по анализу дерева отказов" инструмента методологии электронной оценки безопасности полетов (eSAM) ЕВРОКОНТРОЛЯ: https://www.eurocontrol.int/tool/safety-assessment-methodology.

- Для упрощения рассматривается вектор атаки, ограниченный наземным сегментом инфраструктуры CPDLC: то есть атака, исходящая из наземных средств ПАНО (внутренней сети или серверов), из сети "земля – земля" поставщика услуг связи или из локальной сети и серверов воздушно-наземной станции; иными словами, в примере исключаются другие векторы атаки, такие как передача сообщений CPDLC по линии связи "воздух – земля". Используя пример определения киберугроз, приведенный в добавлении C (см. редакцию настоящего документа для служебного пользования), эту киберугрозу можно классифицировать следующим образом:
  - Сегмент: поставщик аэронавигационного обслуживания.
  - Функция: связь, навигация и наблюдение (CNS).
  - Подфункция: связь.
  - Киберугроза: изменение (модификация содержимого сообщения).

Рис. 3. Угроза: искажение данных
(Примечание. Рис. 4 в редакции для служебного пользования)

ПОЭТАПНОЕ ПРИМЕНЕНИЕ МЕТОДИКИ



⇨ Эксперты по безопасности полетов совместно с экспертами по кибербезопасности провели анализ существующих оценок рисков для безопасности полетов в отношении функции связи "воздух – земля" и определили CPDLC в качестве системы и информации, поддерживающей критически важную функцию, которую необходимо оценить на предмет киберрисков.

- ⇨ Эксперты по безопасности полетов разработали исходную диаграмму дерева отказов [17] систем безопасности без учета каких-либо киберфакторов. Конечным событием, связанным с рассматриваемым сценарием киберугрозы для CPDLC, является "необнаруженная несанкционированная передача одного или нескольких сообщений, использованных для предоставления диспетчерских разрешений одному или нескольким воздушным судам".
- ⇨ **Целевой уровень безопасности полетов для конечного события составляет "не более 10^−5 происшествий за час полета".**

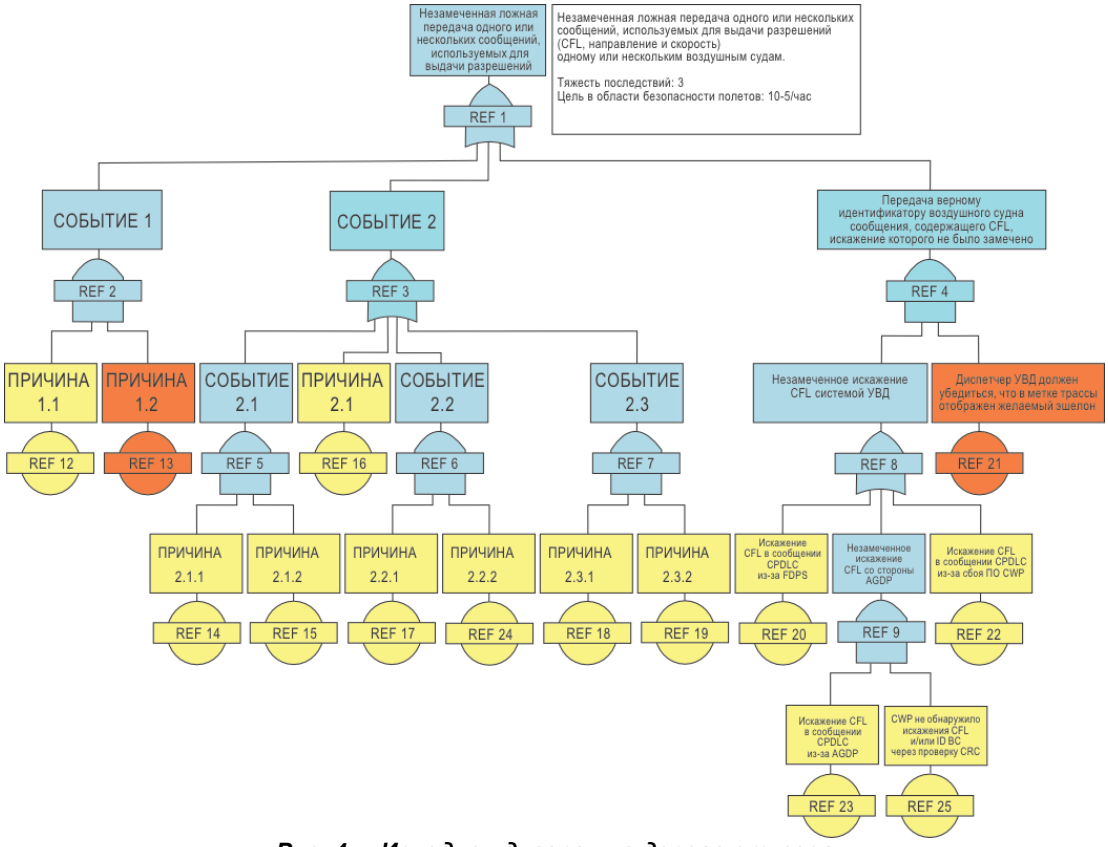
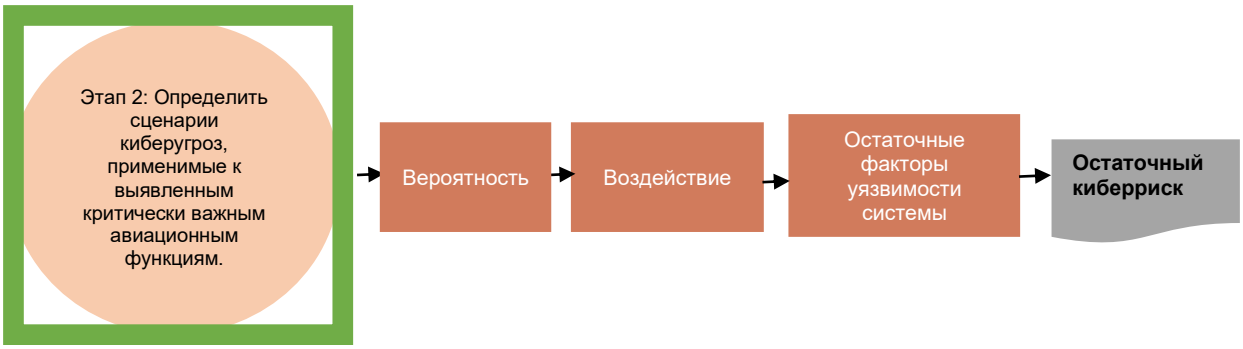


Рис. 4. Исходная диаграмма дерева отказов

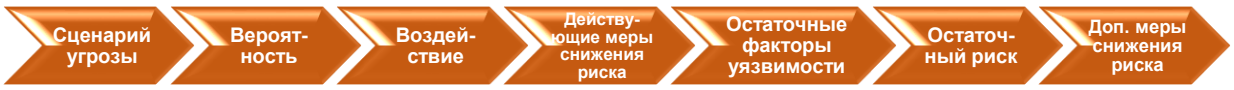
(Примечание. Рис. 5 в редакции для служебного пользования)

17. Акронимы, используемые в диаграмме дерева отказов:
    - AGDP: процессор линии передачи данных "воздух – земля", сервер данных "воздух – земля"
    - CFL: разрешенный эшелон полета
    - CWP: рабочее место диспетчера (человеко-машинный интерфейс)
    - FDPS: система обработки полетных данных



- ⇨ Эксперты по кибербезопасности в сотрудничестве с экспертами по безопасности полетов определили "искажение данных сообщения CPDLC, отправленного авиадиспетчером пилоту" в качестве вероятного сценария киберугрозы, который должен быть оценен и интегрирован в вышеуказанную оценку рисков для безопасности полетов.
- ⇨ Оценка киберрисков была проведена экспертами по кибербезопасности ПАНО в сотрудничестве с экспертами по безопасности полетов. Эксперты по кибербезопасности обладают знаниями об известных методах и векторах кибератаки, в то время как эксперты по безопасности полетов обладают знаниями об архитектуре системы.

Компоненты оценки киберрисков на этапе 2 расширены и включают в себя следующие этапы:



Для проведения оценки киберрисков в целях построения матрицы киберрисков были предприняты следующие шаги.

- ⇨ **Вероятность:**
  - Эксперты в области безопасности полетов часто выражают вероятность в количественных показателях (например, в количестве происшествий за летные часы). Кроме того, при использовании дерева отказов некоторые эксперты используют "расстояние" от конечного события в дереве отказов для оценки вероятности (например, чем дальше находится отказ от конечного события, тем ниже вероятность того, что он приведет к возникновению конечного события и повлияет на достижение целевого уровня безопасности полетов). С другой стороны, эксперты по кибербезопасности часто используют таблицы вероятностей с дискретными значениями (см., например, таблицу 1 в главе 2). Цель этой совместной работы экспертов заключается в том, чтобы согласовать понимание различных компонентов риска.
  - Таким образом, в данном примере включение киберугрозы в дерево отказов (элементы, выделенные красным) облегчает оценку вероятности возможности и намерений субъекта угрозы относительно ее материализации[18].

18. При полной оценке киберрисков к исходной схеме может быть добавлено множество векторов атак. Для простоты в примере приведены только два возможных вектора атаки.

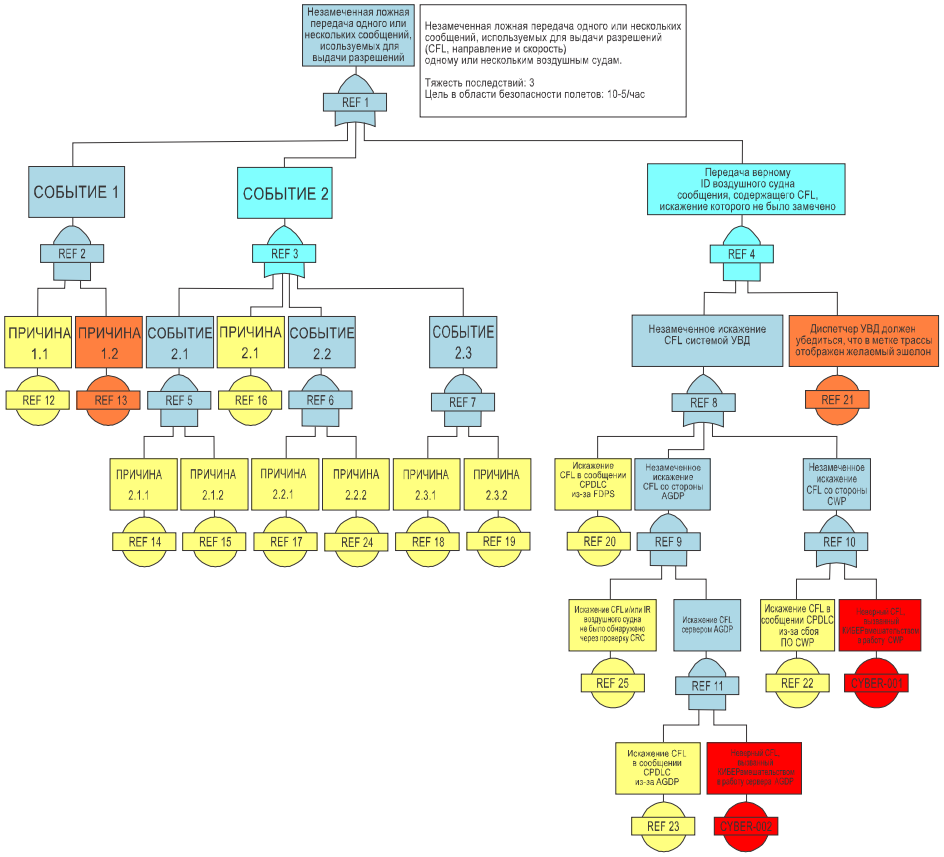


Рис. 5. Обновленная диаграмма дерева отказов
(Примечание. Рис. 6 в редакции для служебного пользования)

- Вероятность киберугрозы была оценена на 2 балла, что соответствует СРЕДНЕ-НИЗКОМУ уровню (т. е. сценарий, примеров которого не существует или нет в практике последнего времени, однако в отношении которого имеются некоторые сведения о намерениях его осуществить, хотя, по всей видимости, методика для успешной реализации нападения отработана еще недостаточно и вполне вероятно, что предпочтение будет отдано другой форме совершения нападения).

⇨ **Воздействие/последствия/эффект**

- Оценка воздействия включает в себя оценку разумного наихудшего сценария, что в данном случае означает, что кибератака была успешной и конечное событие не было предотвращено. Таким образом, в оценке воздействия предполагается максимально возможная серьезность конечного события до возникновения киберугрозы, которая представляет собой и соответствует СРЕДНЕМУ уровню воздействия (значительные последствия для безопасности полетов: "серьезный инцидент, который привел к снижению способности эксплуатационного персонала справляться с неблагоприятными эксплуатационными условиями из-за увеличения рабочей нагрузки или вследствие условий, понижающих эффективность работы").

⇨ **Уязвимость:**

- Оценка уязвимости проводится с учетом существующих мер по снижению риска.
- Относительно этого в FTA указано, что выполняется контроль сообщения CPDLC с использованием циклического избыточного кода (CRC)[19]. Таким образом, он принимается во внимание, равно как и меры, связанные с информационной безопасностью (защита систем и серверов) и авиационной безопасностью (проверка анкетных данных и контроль доступа).

19. CRC определяется как "метод, гарантирующий, что данные не были изменены после отправки по каналу связи". Источник: NIST SP800-72.

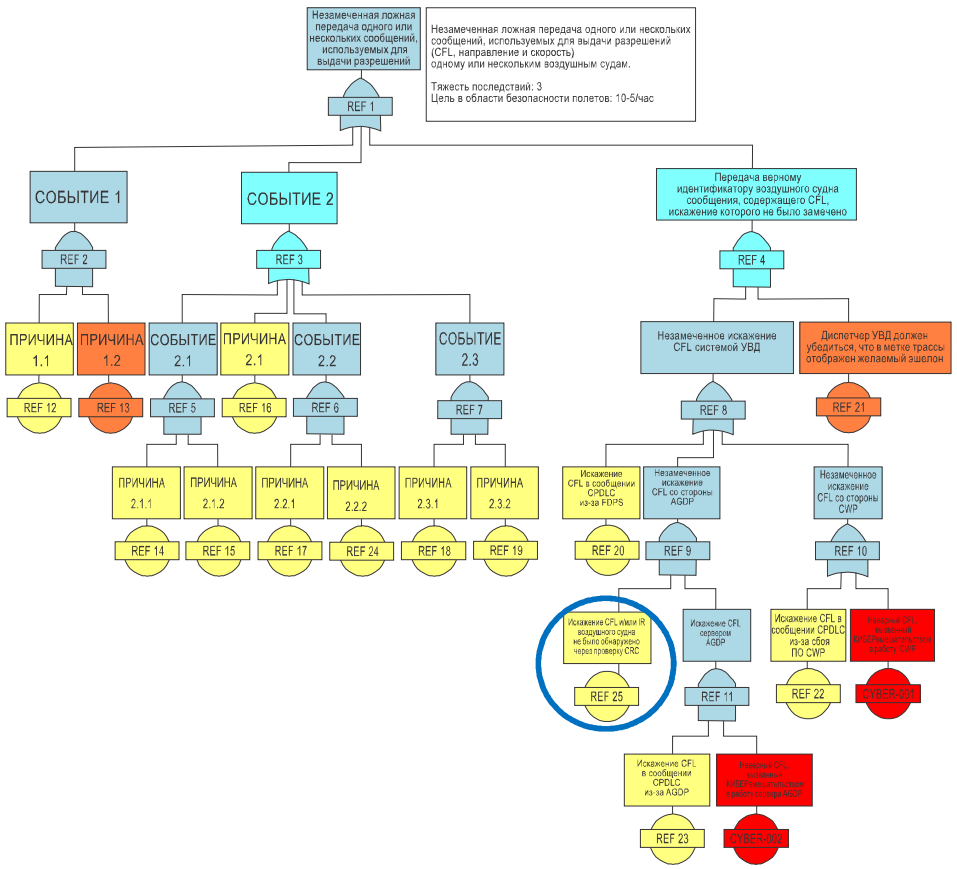


Рис. 6. Обновленная диаграмма дерева отказов (часть диаграммы выделена кругом)
(Примечание. Рис. 7 в редакции для служебного пользования)

- Эксперты по кибербезопасности знают, что CRC в основном используется для обнаружения непреднамеренных ошибок в данных. CRC не эффективен против преднамеренного вмешательства, поскольку субъект атаки может изменить не только само сообщение, но и хэш CRC, в связи с чем эксперты по кибербезопасности пришли к выводу, что существующих средств киберконтроля может быть недостаточно для снижения этого риска.
- Кроме того, оценка уязвимости привела к выводу о том, что внешнюю кибератаку было бы сложно подготовить и осуществить. Сети и системы связи ПАНО надлежащим образом защищены от внешних атак, и в организации обеспечены достаточные возможности мониторинга и обнаружения. Внутреннюю атаку (внутреннюю угрозу) было бы относительно легче организовать, поскольку применяемые меры физической безопасности также достаточны (контроль доступа в соответствующие помещения и проверка анкетных данных персонала, имеющего доступ к этим зонам).
- Соответственно, уязвимости присваивается СРЕДНЕ-ВЫСОКИЙ уровень (0,8).

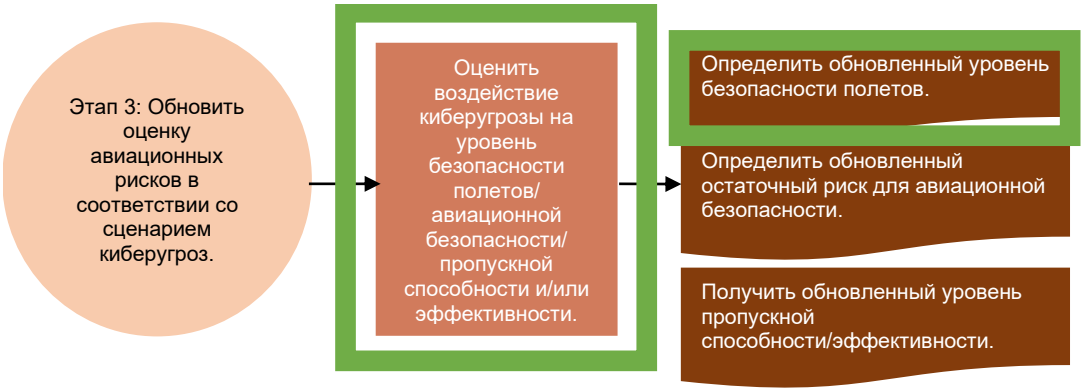
⇨ **Остаточный киберриск:**

- Остаточный киберриск теперь можно рассчитать путем перемножения оценок вероятности, воздействия и уязвимости: **2 x 3 x 0,8 = 4,8**.

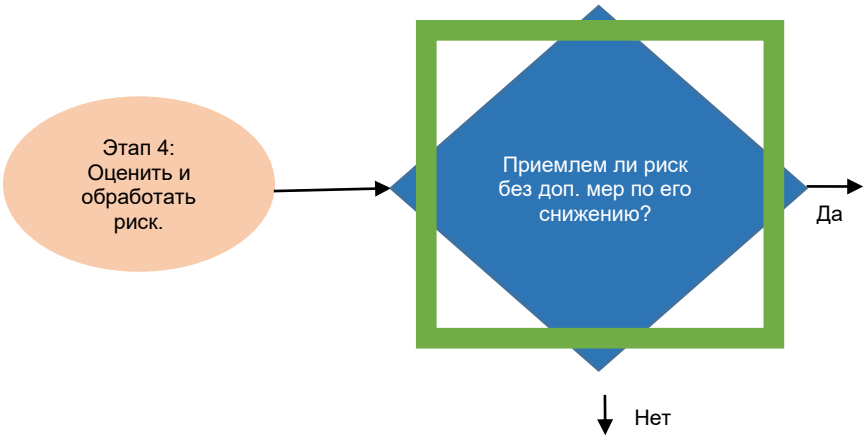
⇨ Балльная оценка остаточного киберриска (4,8) была округлена до 5, поскольку эксперты посчитали, что она ближе к СРЕДНЕ-НИЗКОЙ, чем к НИЗКОЙ.

Таким образом, матрица киберрисков будет выглядеть следующим образом:

МАТРИЦА КИБЕРРИСКОВ					
Сценарий	**Вероятность**	**Воздействие**	**Меры снижения риска**	**Факторы уязвимости**	**Остаточный фактор риска**
Постороннее лицо вмешивается в полезную нагрузку данных сообщения CPDLC, отправленного диспетчером пилоту.	**Балл = 2** СРЕДНЕ-НИЗКИЙ уровень Сценарий, примеров которого не существует или нет в практике последнего времени, однако в отношении которого имеются некоторые сведения о намерениях его осуществить, хотя, по всей видимости, методика для успешной реализации нападения отработана еще недостаточно и вполне вероятно, что предпочтение будет отдано другой форме совершения нападения.	**Балл = 3** ЗНАЧИТЕЛЬНЫЙ уровень Конечное событие для безопасности полетов: Необнаруженная несанкционированная передача одного или нескольких сообщений, использованных для предоставления диспетчерских разрешений.	CRC Возможности мониторинга и обнаружения проникновения посторонних лиц уже реализованы. Меры обеспечения безопасности информационных систем Контроль физического доступа и проверка анкетных данных	**Балл = 0,8** СРЕДНЕ-ВЫСОКИЙ уровень CRC не является подходящим инструментом для обнаружения злонамеренного искажения информации, поскольку он может быть искажен вместе с передаваемой информацией.	**Балл = 4,8 (округлен до 5)** СРЕДНЕ-НИЗКИЙ уровень Эта оценка будет сравниваться с оценками других сценариев угроз и использоваться для ранжирования угроз.



- ⇨ Теперь, когда диаграмма дерева отказов обновлена и организация располагает гораздо большей информацией о киберугрозе, преобразованной в киберриск и соотнесенной с целями в области безопасности полетов, первоначальная оценка риска для безопасности полетов может быть обновлена с учетом оценки этой киберугрозы, что потенциально может привести к изменению вероятности возникновения конечного события в области безопасности полетов ("необнаруженная несанкционированная передача одного или нескольких сообщений, использованных для предоставления диспетчерских разрешений").
- ⇨ Это послужит основой для следующих этапов: оценки риска и его обработки.



ПАНО использует уже имеющуюся у него матрицу приемлемости рисков с учетом обновленных оценок. Эта матрица может содержать различные типы критериев, такие как:

- критерии кибербезопасности, источники которых включают в себя авиационное регулирование, нормы/законы о критически важной инфраструктуре, допустимый для организации уровень риска и т. д.;
- критерии безопасности полетов, которые включают в себя взаимосвязь между воздействием на безопасность и целевой с точки зрения безопасности полетов вероятностью, а также источники, связанные с соответствующим авиационным регулированием;
- критерии пропускной способности и эффективности аэронавигации, которые зависят от организации (и выходят за рамки данного примера).

Эта оценка, проведенная в соответствии с установленными организационными критериями, должна привести к принятию решения: **может ли риск быть принят как есть, или следует принять меры по снижению киберриска в дополнение к существующим средствам контроля?**

По итогам оценки было принято решение о том, что, несмотря на то, что остаточный киберриск оценивается как СРЕДНЕ-НИЗКИЙ, необходимо рассмотреть вопрос о принятии дополнительных мер, которые могли бы еще больше снизить риск.

⇨ **Меры по снижению рисков для кибербезопасности:**

- Киберэксперты предложили в первую очередь добавить новое оборудование для дополнительной защиты системы от помех. Однако предложение добавить новое оборудование было отклонено экспертами по безопасности полетов, поскольку это создало бы новые точки отказа, которые потребовали бы пересмотра всей оценки безопасности системы, а также других затронутых систем.
- Эксперты по безопасности полетов и эксперты по кибербезопасности пришли к общему мнению, что имеющиеся средства контроля для защиты системы от внешних кибератак достаточны, и в связи с этим решили искать меры по снижению риска внутренней угрозы, которая в ходе оценки киберрисков была признана более вероятной.
- Эксперты по кибербезопасности предложили меры, которые ужесточают привилегии доступа к соответствующим компьютерам и серверам, и это предложение было принято.

⇨ **Дополнительные меры по снижению риска**

- С помощью этих мер по снижению рисков для кибербезопасности было установлено, что данный риск может быть дополнительно снижен путем применения других типов мер.
- Эксперты по авиационной безопасности предложили ввести более строгие проверки анкетных данных и меры контроля доступа для персонала, имеющего доступ к помещениям, из которых производится УВД, и серверным комнатам.
- Оценка риска была произведена повторно с учетом новых мер по снижению риска (как кибермер, так и мер в области авиационной безопасности), и было решено, что новые меры снизят риск до приемлемого уровня, таким образом применение было утверждено.

⇨ **Матрица киберрисков**

- Это привело к расширению матрицы оценки киберрисков путем включения в нее дополнительных мер по их снижению, зафиксированных для последующего внедрения. Окончательная матрица оценки киберрисков приведена ниже.

МАТРИЦА КИБЕРРИСКОВ						
Сценарий	**Вероятность**	**Воздействие**	**Меры снижения риска**	**Факторы уязвимости**	**Остаточный фактор риска**	**Дополнительные меры по снижению риска**
Постороннее лицо вмешивается в полезную нагрузку данных сообщения CPDLC, отправленного диспетчером пилоту.	**Балл = 2** СРЕДНЕ-НИЗКИЙ уровень Сценарий, примеров которого не существует или нет в практике последнего времени, однако в отношении которого имеются некоторые сведения о намерениях его осуществить, хотя, по всей видимости, методика для успешной реализации нападения отработана еще недостаточно и вполне вероятно, что предпочтение будет отдано другой форме совершения нападения.	**Балл = 3** ЗНАЧИТЕЛЬНЫЙ уровень Конечное событие для безопасности полетов: Необнаруженная несанкционированная передача одного или нескольких сообщений, использованных для предоставления диспетчерских разрешений.	CRC Возможности мониторинга и обнаружения проникновения посторонних лиц уже реализованы. Меры обеспечения безопасности информационных систем Контроль физического доступа/проверка анкетных данных	**Балл = 0,8** СРЕДНЕ-ВЫСОКИЙ уровень CRC не является подходящим инструментом для обнаружения злонамеренного искажения информации, поскольку он может быть искажен вместе с передаваемой информацией.	**Балл = 4,8 (округлен до 5)** СРЕДНЕ-НИЗКИЙ уровень Эта оценка будет сравниваться с оценками других сценариев угроз и использоваться для ранжирования угроз.	**Кибербезопасность: Оптимизация и мониторинг привилегий цифрового доступа на соответствующих компьютерах и серверах.** **Прочее: Более строгие проверки анкетных данных и меры контроля физического доступа для персонала, имеющего доступ к помещениям, из которых производится УВД, и серверным комнатам**.

ВЫВОД

В этом примере в иллюстративных целях приведен пошаговый подход, чтобы показать, как должны взаимодействовать оценки рисков для безопасности полетов и киберрисков для борьбы с киберугрозами и рисками для гражданской авиации. На практике этот процесс носил бы более постепенный и комплексный характер в зависимости от организационной структуры управления и действующей нормативно-правовой базы.

— — — — — — — —

Добавление B

ПРИМЕР ПРИМЕНЕНИЯ МЕТОДИКИ В ОБЛАСТИ УПРАВЛЕНИЯ РИСКАМИ ДЛЯ АВИАЦИОННОЙ БЕЗОПАСНОСТИ

ДОПУЩЕНИЯ И ОБЩАЯ ИНФОРМАЦИЯ

Пример, приведенный ниже, иллюстрирует интеграцию оценки киберрисков в оценку рисков для авиационной безопасности с использованием гипотетического сценария угрозы, оцениваемого государством.

Допущения:

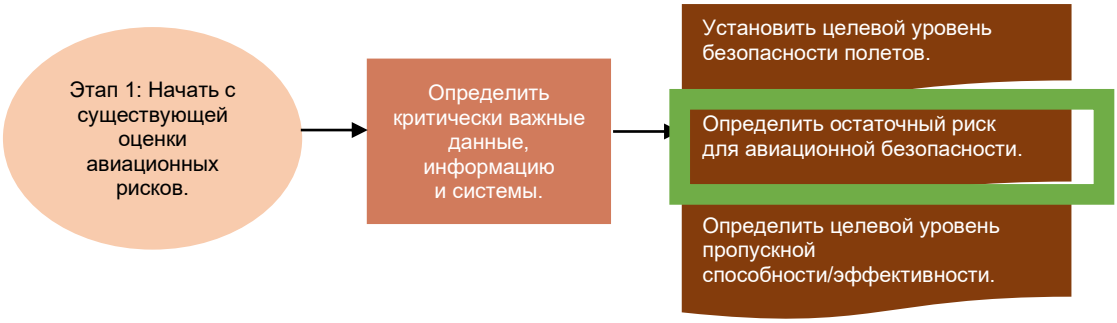
- Государство уже провело качественную и количественную оценку рисков для авиационной безопасности и снизило эти риски с помощью матриц рисков для авиационной безопасности.
- Эксперты по авиационной безопасности определили досмотр ручной клади в качестве одной из критически важных авиационных функций.
- Для упрощения допускается, что оцениваемая киберугроза влияет только на авиационную безопасность (и не влияет на безопасность полетов и на эффективность и/или пропускную способность аэронавигации).
- Государство использует те же таблицы оценки вероятности, воздействия и уязвимости, которые использованы в данном документе.
- В целях единообразия для балльной оценки, применяемой при оценке киберрисков, используются те же значения, что и в главе 3 настоящего документа в редакции для служебного пользования. Однако на практике балльные оценки вероятности, воздействия и уязвимости будут различаться для разных государств и организаций в зависимости от разных переменных, влияющих на эти оценки (возможностей, намерения, существующих мер по снижению риска и т. д.).
- В связи с чувствительностью оценки рисков авиационной безопасности здесь описывается только процесс интеграции оценки киберрисков в оценку авиационной безопасности. Процесс оценки киберрисков описан в подробностях.

Сценарий киберугрозы:

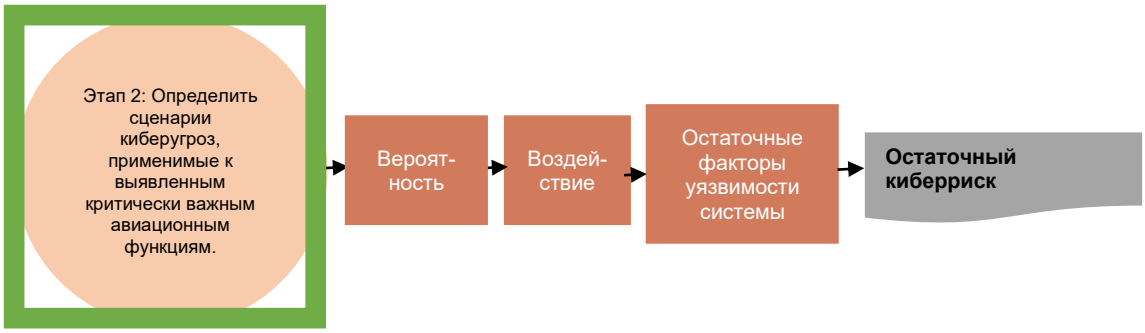
- Государство анализирует различные возможные методы и приемы противника, пытающегося пронести на борт в ручной клади самодельные взрывные устройства (PBIED) с намерением вызвать крушение воздушного судна.
- Эксперты по авиационной безопасности совместно с экспертами по кибербезопасности провели анализ существующих оценок рисков для AVSEC в отношении досмотра ручной клади и определили обнаруживающий компонент оборудования для досмотра в качестве системы и информации (поддерживающих критически важную авиационную функцию), которые необходимо оценить на предмет киберрисков.
- Эксперты по авиационной безопасности использовали проведенную ранее оценку рисков для авиационной безопасности, связанных с PBIED (перевозимыми на теле или в ручной клади), и в рамках данной работы рассмотрели только провоз PBIED в ручной клади.
- В ходе обсуждений с экспертами по авиационной безопасности эксперты по кибербезопасности определили "искажение данных компонента обнаружения с целью изменения результатов автоматизированного процесса досмотра" в качестве сценария киберугрозы, подлежащего оценке и включению в вышеуказанную оценку рисков для авиационной безопасности.
- Вектор атаки: эта атака может быть осуществлена путем вмешательства в работу оборудования для досмотра по обнаружению посредством получения физического или удаленного доступа к этому оборудованию.
- Используя пример определения киберугроз, приведенный в добавлении C (см. редакцию настоящего документа для служебного пользования), эту киберугрозу можно классифицировать следующим образом:
  - Сегмент: аэропорт.
  - Функция: авиационная безопасность.

- Подфункция: досмотр ручной клади.
- Киберугроза: изменение (вмешательство в работу программного обеспечения/систем обнаружения).

ПОЭТАПНОЕ ПРИМЕНЕНИЕ МЕТОДИКИ

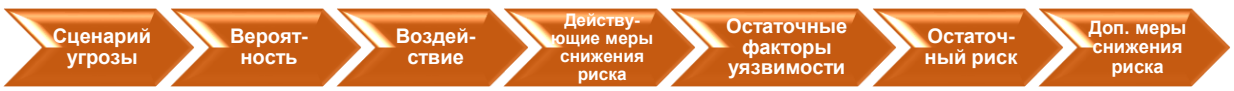


- ⇨ Эксперты по авиационной безопасности совместно с экспертами по кибербезопасности провели анализ существующих оценок рисков для авиационной безопасности в отношении самодельных взрывных устройств, перевозимых человеком в ручной клади, и определили обнаруживающий компонент оборудования для досмотра в качестве системы и информации, поддерживающих критически важную авиационную функцию и подлежащих оценке на предмет киберрисков.
- ⇨ Эксперты по авиационной безопасности провели первоначальную оценку риска PBIED без учета каких-либо киберфакторов. Сценарий авиационной безопасности, связанный с рассматриваемым сценарием киберугрозы, выглядит так: "Пронос пассажиром на борт запрещенного предмета с намерением вызвать крушение воздушного судна ".
- ⇨ **Результатом этого процесса является получение остаточного риска безопасности для описанного выше сценария.**



- ⇨ Эксперты по кибербезопасности совместно с экспертами по авиационной безопасности определили "искажение данных компонента обнаружения с целью изменения результатов процесса досмотра" в качестве вероятного сценария киберугрозы, подлежащего оценке и включению в вышеуказанную оценку рисков для авиационной безопасности.
- ⇨ Оценка киберрисков была проведена экспертами по кибербезопасности государства в сотрудничестве с экспертами по авиационной безопасности. Эксперты по кибербезопасности обладают знаниями об известных методах проведения кибератак и векторах кибератаки, в то время как эксперты по авиационной безопасности — об оборудовании и его допустимых параметрах.

Компоненты оценки киберрисков на этапе 2 расширены и включают в себя следующие этапы:



Для проведения оценки киберрисков для авиационной безопасности в целях построения матрицы киберрисков были предприняты следующие шаги.

- ⇨ **Вероятность:**
  - Как эксперты по авиационной безопасности, так и эксперты по киберугрозам часто используют таблицы вероятностей с дискретными значениями (как, например, таблица 1 в главе 2), которые помогают согласовать понимание различных компонентов риска.
  - Для того чтобы сделать осуществление оцениваемой кибератаки возможной, потребовалась бы тщательная подготовка.
  - Внешняя атака сложна в осуществлении, поскольку оборудование для досмотра либо является автономным (не подключенным к сети), либо подключено к локальной закрытой сети, что потребовало бы больших усилий и ноу-хау для изменения результата процесса досмотра.
  - Внутренняя угроза возможна, но для изменения результатов процесса досмотра потребовалось бы много усилий и ноу-хау, например:
    - детальное знание аэропорта, пунктов досмотра, расписания и т. д.;
    - высокая степень взаимодействия (атака не может быть осуществлена без посторонней помощи);
    - доступ к оборудованию и/или к локальной сети.
  - Имеются свидетельства наличия в настоящее время умысла.
  - В связи с этим вероятность киберугрозы была установлена на уровне 3, что соответствует СРЕДНЕМУ уровню (т. е. в большой степени вероятный сценарий, так как есть некоторые сведения о намерениях и способности совершить атаку, и возможно есть некоторые примеры).

- ⇨ **Воздействие/последствия/эффект**:
  - Оценка воздействия включает в себя оценку разумного наихудшего сценария, что в данном случае означает, что кибератака была успешной.
  - Результатом кибератаки стал бы искаженный результат досмотра, в котором, возможно, отсутствовали бы запрещенные предметы. Это может привести к крушению воздушного судна, сотням погибших, в том числе, возможно, на земле. Еще одним последствием был бы очень большой непосредственный ущерб и долгосрочный экономический ущерб. Таким образом, уровень воздействия был бы ВЫСОКИМ (5 баллов).

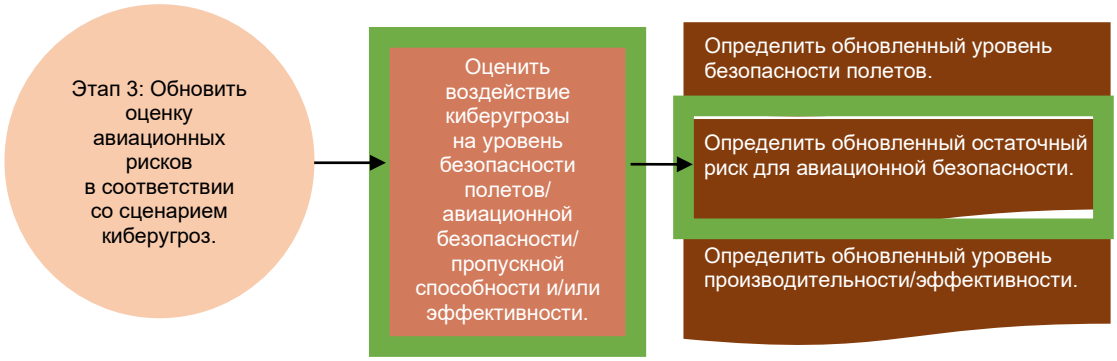
- ⇨ **Уязвимость:**
  - Оценка уязвимости проводится с учетом существующих мер по снижению риска.
  - Применительно к существующим мерам по снижению риска:
    - государство предписало применять Стандарты и Рекомендуемую практику (SARPS) Приложения 17 *"Авиационная безопасность"* в отношении досмотра пассажиров с использованием систем обнаружения, установленных в аэропорту;
    - государство требует также от своих эксплуатантов внедрения Стандарта 4.9.1 и Рекомендуемой практики 4.9.2, касающихся противодействия киберугрозам, в связи с чем аэропорт принимает следующие меры:
      - в ИТ-сетях реализовано логическое [20] или физическое разграничение с коммерческой и эксплуатационной инфраструктурой;
      - в отношении персонала проводятся проверки анкетных данных, а также принимаются меры авиационной безопасности для защиты доступа к оборудованию.
  - Эксперты в области кибербезопасности подтвердили, что существующие меры контроля достаточны для снижения данного киберриска. Однако, поскольку эксперты по авиационной безопасности знают, что требования, внедряемые аэропортом, не всегда выполняются во всем мире (особенно те, которые связаны с Рекомендуемой практикой), было решено оценить уязвимость как СРЕДНЕ-НИЗКУЮ (0,4).

- ⇨ **Остаточный киберриск:**
  - Остаточный киберриск теперь можно рассчитать путем перемножения оценок вероятности, воздействия и уязвимости: **3 x 5 x 0,4 = 6, что позволяет оценить остаточный киберриск как СРЕДНЕ-НИЗКИЙ**.

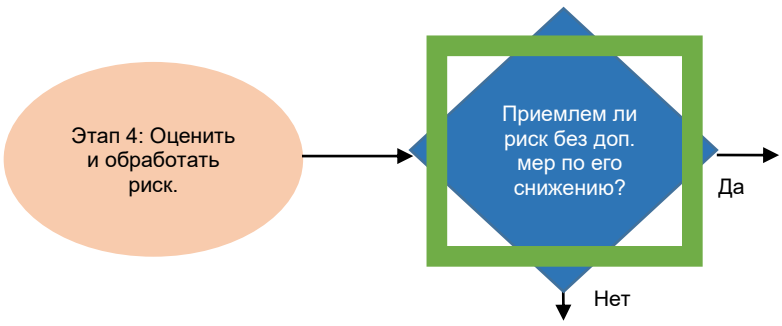
20. Под логическим разделением понимается сегментация сети путем создания логических (виртуальных) зон в одной физической сети или аппаратном элементе.

Теперь матрица киберрисков выглядит следующим образом:

МАТРИЦА КИБЕРРИСКОВ					
Сценарий	**Вероятность**	**Воздействие**	**Меры снижения риска**	**Факторы уязвимости**	**Остаточный фактор риска**
Пронос пассажиром на борт запрещенного предмета с целью вызвать крушение воздушного судна путем изменения результатов работы средств досмотра.	**Балл = 3** СРЕДНИЙ Способен ли противник на такие действия? Есть ли заинтересованность в атаке на объект гражданской авиации?	**Балл = 5** ВЫСОКИЙ При разумном наихудшем сценарии: сколько будет погибших? Ожидается ли нанесение ущерба инфраструктуре? Потеряет ли общественность доверие к авиаперевозкам? Каким будет экономический ущерб?	Приложение 17, Стандарт 4.9.1 и Рекомендуемая практика 4.9.2 применяются к досмотру пассажиров с использованием систем обнаружения.	**Балл = 0,4** СРЕДНЕ-НИЗКИЙ уровень Каков вывод относительно уязвимости авиации к этому сценарию угрозы по итогам рассмотрения действующих мер по снижению последствий?	**Балл = 6** Эта оценка будет сравниваться с оценками других сценариев угроз и использоваться для ранжирования угроз.



- После того как киберугроза была преобразована в киберриск, соответствующий целям в области авиационной безопасности, первоначальная оценка риска для авиационной безопасности может быть обновлена путем включения в нее оценки киберугрозы, которая теперь фигурирует в матрице рисков для авиационной безопасности в отношении рассматриваемого сценария, что потенциально может привести к возникновению нового остаточного риска для авиационной безопасности.
- Это послужит основой для следующих этапов: оценки риска и его обработки.



- ⇨ На основе этих данных государство обновит свою матрицу рисков, связанных с PBIED, включив в нее этот способ совершения атаки.

Результатом этой оценки должно стать решение: **может ли риск быть принят как есть, или следует реализовать меры по снижению киберугрозы в дополнение к существующим мерам контроля?**

- ⇨ Был сделан вывод о том, что остаточный киберриск слишком низок для того, чтобы изменить первоначальную оценку, в связи с чем остаточный риск общего сценария угрозы типа PBIED не подвержен влиянию данного сценария киберугрозы (то есть угроза для авиационной безопасности остается на прежнем, более высоком уровне).
- ⇨ Эксперты по кибербезопасности сочли также удовлетворительными существующие меры контроля, поддерживающие надежность процесса досмотра.
- ⇨ В то же время эксперты по кибербезопасности отметили, что любое изменение оборудования требует повторной сертификации оборудования соответствующим органом, что может сделать систему уязвимой для будущих киберугроз, если обнаруженные факторы уязвимости не будут своевременно устранены. В связи с этим был начат проект по поиску сбалансированного подхода между сертификацией и обновлением средств контроля за кибербезопасностью на оборудовании для досмотра, и результат проекта был зарегистрирован в качестве дополнительной меры для реализации в дальнейшем в поддержку снижения киберрисков.
- ⇨ Обновленная матрица киберрисков для этого сценария приведена далее.

МАТРИЦА КИБЕРРИСКОВ

Сценарий	Вероятность	Воздействие	Меры снижения риска	Факторы уязвимости	Остаточный фактор риска	Дополнительные меры по снижению риска
Пронос пассажиром на борт запрещенного предмета с намерением вызвать крушение воздушного судна путем изменения результатов работы средств досмотра.	**Балл = 3** СРЕДНИЙ Способен ли противник совершить такие действия? Есть ли заинтересованность в атаке на объект гражданской авиации?	**Балл = 5** ВЫСОКИЙ При разумном наихудшем сценарии: сколько будет погибших? Ожидается ли нанесение ущерба инфраструктуре? Потеряет ли общественность доверие к авиаперевозкам? Каким будет экономический ущерб?	Приложение 17, Стандарт 4.9.1 и Рекомендуемая практика 4.9.2 применяются к досмотру пассажиров с использованием систем обнаружения.	**Балл = 0.4** СРЕДНЕ-НИЗКИЙ уровень После рассмотрения действующих мер по снижению последствий, насколько авиация уязвима к этому сценарию угрозы?	**Балл = 6** Эта балльная оценка будет сравниваться с балльной оценкой, выведенной для других сценариев угроз, и использоваться для ранжирования угроз.	Разработка процессов, обеспечивающих баланс между исправлением факторов уязвимости и повторной сертификацией оборудования для досмотра ручной клади.

ВЫВОД

В этом примере в иллюстративных целях приведен пошаговый подход, чтобы показать, как должны взаимодействовать оценки рисков для авиационной безопасности и киберрисков, чтобы сделать возможной борьбу с киберугрозами и рисками для гражданской авиации. На практике этот процесс носил бы более постепенный и комплексный характер в зависимости от государственной или организационной структуры управления и действующей нормативно-правовой базы.

— КОНЕЦ —

ISBN 978-92-9275-973-5